

Constituency casework of Members of Parliament and the processing of sensitive personal data

Data Protection Act

Contents

Introduction.....	2
Overview	2
What the DPA says	3
Schedule 2 condition for processing	4
Schedule 3 condition for processing	4
The Data Protection (Processing of Sensitive Personal Data)(Elected Representatives) Order 2002	6
Other considerations.....	7
More information	7

Introduction

Update

This guidance has been updated to include boxes that signpost key changes in the new data protection regime that will affect political campaigning from 25 May 2018 onwards, and link to new sources of relevant GDPR guidance.

We will be updating this guidance in more detail in due course.

For more information on the GDPR, see our [Guide to the GDPR](#).

The transition period for leaving the EU ended on 31 December 2020. The GDPR has been retained in UK law as the UK GDPR, and will continue to be read alongside the Data Protection Act 2018, with technical amendments to ensure it can function in UK law. We will be updating this guidance in more detail in due course. For more information on the UK GDPR, see our [Guide to the UK GDPR](#)

1. The Data Protection Act 1998 (DPA) is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.
2. An overview of the main provisions of the DPA can be found in [The Guide to Data Protection](#).
3. This is part of a series of guidance, which goes into more detail than the Guide, to help data controllers to fully understand their obligations and promote good practice.
4. This guidance provides advice for Members of Parliament, and data controllers contacted by Members of Parliament, on the processing of sensitive personal data in connection with constituency casework.

Overview

- In carrying out constituency casework, Members must ensure that they can satisfy the conditions for processing required by the first data protection principle.
- For non-sensitive personal data, Members can usually rely on the implied consent of the constituent as providing the necessary condition.
- For sensitive personal data, members can usually rely on the The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002, which also covers the disclosure of such data by organisations responding to Members.
- There may still be circumstances where it is necessary to contact the constituent to obtain consent to process their sensitive personal data.

Update

The UK GDPR requires that personal data are processed fairly, lawfully and in a transparent manner. This builds on existing requirements under the Data Protection Act 1998. Individuals have the right to be informed about the collection and use of their personal data. You must provide individuals with privacy information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with.

See our guidance on the [right to be informed](#) for further details.

What the DPA says

5. The first data protection principle says that:

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

- a) at least one of the conditions in Schedule 2 is met, and
- b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

6. Members should first ensure that the processing of personal data is fair and lawful. This should normally be straightforward

in circumstances where a constituent asks a Member to assist them in resolving a problem. Further information on the requirement to process personal data fairly and lawfully can be found in the Guide to Data Protection.

7. This guidance concentrates on the element of the first data protection principle concerning the conditions for processing found in Schedules 2 and 3.

Schedule 2 condition for processing

Update

Consent is likely to remain a valid lawful basis for processing personal data as part of constituency casework where it does not constitute special category or criminal conviction data. However other lawful bases may also be available. You can get more [information about all the lawful bases in our Guide to the UK GDPR](#).

8. For the purposes of a Member processing personal data in relation to constituency casework, consent will be the relevant Schedule 2 condition in most instances. In the context of Schedule 2, implied consent is a valid form of consent.
9. Consent can be implied from a relevant action, in this case the raising of the matter by a constituent with the Member in the expectation that his or her personal data will be further processed by the Member and relevant third party organisations. The constituent will expect that the Member will retain any personal information provided, will disclose it as appropriate and that organisations involved in the matter will disclose personal information to Members where this is necessary to provide an appropriate response.
10. However, there may be circumstances where the processing will go beyond the expectation of the constituent, or where there is uncertainty over the constituent's wishes. In cases like this it would be appropriate to go back to the constituent to make sure consent is in place.

Schedule 3 condition for processing

Update

Under the UK GDPR you need to satisfy additional conditions in order to process special category or criminal conviction data. This is similar to the requirements under the Data Protection Act 1998 to satisfy Schedule 3 conditions in respect of sensitive personal data.

See our [Guide to UK GDPR](#) for further information on [special category](#) and [criminal conviction data](#).

11. In cases involving sensitive personal data, a condition in Schedule 3 is also required.
12. The DPA defines “sensitive personal data” as information about an individual’s:
 - racial or ethnic origin;
 - political opinions;
 - religious beliefs;
 - trade union membership;
 - health;
 - sexual life;
 - alleged criminal activity; or
 - court proceedings.
13. Consent is also available as a processing condition in schedule 3. However, the requirement is for it to be “explicit”, which means that a constituent must consent to a specific act of processing. If explicit consent is given, it follows that consent for the purposes of Schedule 2 is also met.
14. In the past explicit consent was an issue for organisations (such as a local authority) approached by a Member on behalf of a constituent, as this required the constituent to expressly agree to the disclosure by the organisation to the Member. Sometimes evidence was requested in the form of a signed consent form or a formal assurance from the Member that such consent had been given. [The Data Protection \(Processing of](#)

[Sensitive Personal Data\)\(Elected Representatives\) Order 2002](#) addresses this problem.

The Data Protection (Processing of Sensitive Personal Data)(Elected Representatives) Order 2002 ("the Order").

Update

The substantial public interest conditions in clauses 23 and 24 of the draft [Data Protection Bill](#) mirror those in the 2002 Order under the Data Protection Act 1998. If you currently rely upon the 2002 Order conditions to process sensitive personal data then these clauses in the DP Bill are also likely to be applicable and satisfy the requirements of Articles 9 and 10 of the UK GDPR for any special category or criminal conviction data you process for constituency casework.

15. The Order provides an additional Schedule 3 condition so that explicit consent is not always needed when a Member processes sensitive personal data in connection with constituency casework.
16. The Order provides a basis for:
 - Processing of sensitive personal data by Members in connection with their functions as representative, including the disclosure of such information where necessary; and
 - Disclosure of sensitive personal data by organisations responding to Members acting on behalf of individual constituents.
17. The Order does not place an obligation on organisations to disclose sensitive personal data to Members who raise matters on behalf of constituents. However, it provides a legal basis for doing so and removes unnecessary bureaucracy and delay.
18. Members are reminded that, even though a Schedule 3 condition is satisfied, the processing must also be fair and lawful. However, in the great majority of cases organisations will be able to release sensitive personal information about the particular constituent to the Member without advising the constituent of this, provided the disclosure is reasonable and necessary.
19. In exceptional circumstances an organisation responding to a Member may need to contact the constituent to inform them of

a planned disclosure. For example, where an organisation intends to disclose particularly sensitive information which could cause distress to the individual. In such circumstances the obligation to process fairly and lawfully – which includes respecting a duty of confidentiality – could mean that the individual should be alerted to the intended disclosure and consent obtained.

Other considerations

20. Members should think carefully about the security arrangements for sensitive personal data. This should include the arrangements for holding the data and its secure disposal. Further [guidance on security](#) is contained in the Guide to Data Protection on the ICO website.
21. Members are advised to ensure that use of the Order is proportionate, and that individual constituents and others do not feel that their privacy is being negatively affected. Members are asked to inform the Lord Chancellor or the Commissioner of any cases where a constituent is unhappy about disclosures of sensitive personal information made in the course of constituency casework, whether by Members or organisations responding to them.

More information

22. Members will be aware that House officials have, in consultation with the Commissioner's office, produced detailed [guidance](#) on the implications of the DPA for their work.
23. Additional guidance is also available on [our guidance pages](#) if you need further information on other parts of the DPA.
24. If you need any more information about this or any other aspect of data protection, please [contact us](#), or visit our website at www.ico.org.uk.